(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/120004 A1

(51) International Patent Classification[7]: H04L 29/06

(21) International Application Number:
PCT/EP2005/051546

(22) International Filing Date: 7 April 2005 (07.04.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
04102532.1 4 June 2004 (04.06.2004) EP

(71) Applicant *(for all designated States except US)*: INTERNATIONAL BUSINESS MACHINES CORPORATION; New Orchard Road, Armonk, NY 10504 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **RAISCH, Christoph** [DE/DE]; Friedrich-Schaffert-Strasse 21, 70839 Gerlingen (DE). **KRAEMER, Marco** [DE/DE]; Eltinger Str. 87, 70195 Stuttgart (DE). **KIESEL, Sebastian** [DE/DE]; Ostendstr. 44, 70188 Stuttgart (DE). **HAUSER, Christian** [DE/DE]; Federstr. 21, 72116 Moessingen (DE).

(74) Agent: TEUFEL, Fritz; Postal Code, 70548 Stuttgart (DE).

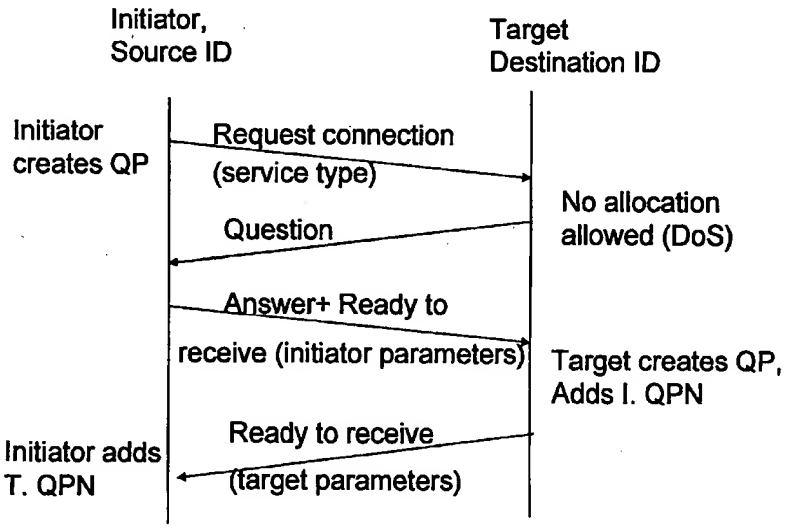
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHOD FOR PROTECTING AGAINST ATTACKS IN A HIGH-SPEED NETWORK



(57) Abstract: A method, module and computer program for protecting a target against attacks in a high-speed network. The method according to the invention comprises the steps of generating a question, after having received a request from an initiator identified by a sourceID associated to a certain node in the network, sending the question to the node identified by the sourceID, in case that an answer to the question is received, evaluating the answer, and in case that a proper answer has been received, enabling communication between the initiator and the target by sending a further message from the target to the initiator.

WO 2005/120004 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

D E S C R I P T I O N

Method for protecting against attacks in a high-speed network

FIELD OF THE INVENTION

The present invention relates to the field of protecting against attacks in a high-speed network and more particularly, to a method and a module for protecting a target in a high-speed network against attacks. The invention further relates to a computer program product with a computer-readable medium and a computer program stored on the computer-readable medium with program coding means which are suitable for carrying out such a method when the computer is run on a computer. Moreover, the invention relates to a method for handling requests in a high-speed network.

DESCRIPTION OF THE RELATED ART

In high-speed networks data exchange is performed based on standarized protocols like TCP/IP or InfiniBand. Communication between nodes in such networks is initiated by so-called handshake protocols which ensure a correct data transfer between the involved network nodes. In this way, certain nodes in a network the so-called initiators are enabled to use services provided by other nodes, hereinafter denoted as targets. Therefore, the initiator sends a request to a target offering a service required by the initiator.

Attacks in networks such as denial of service attacks are characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. This

can be archieved by using a false address or sourceID, respectively and flooding a target in the network by sending a lot of requests which need resources, thereby preventing the server from doing meaningful work.

Denial-of-service attacks can result in significant loss of time and money for many organizations using the network.

A known method uses a 4-way handshake protocol including an initiating message containing certain parameters, a first question message, a answer to the question containing the said parameters and a final message. However, this solution does not effectively prevent a flooding attack for protocols that rely on a predefined sequence of handshake messages.

SUMMARY OF THE INVENTION

It is an object of the invention to provide a method and a module for protecting targets against attacks in high-speed networks which overcome the disadvantages known in the prior art. More particularly, it is an object of the invention to provide a method for handling requests in a high-speed network protecting targets in the network against attacks and consequently, ensuring a unrestricted availability of all services in that network.

These objects are achieved by proposing a method for protecting against attacks in a high-speed network with the features of claim 1, a module for protecting against attacks in a high-speed network with the features of claim 9 and a method for handling requests in a high-speed network according to claim 16.

According to the present invention, a method for protecting a target against attacks in a high-speed network is proposed, said method comprises the steps of generating a question, after having received a request from an initiator identified by a sourceID associated to a certain node in the network, sending the question to the node identified by the sourceID, subsequently, in case that an answer to the question is received, evaluating the question, and in case that a proper answer has been received, enabling communication between the initiator and the target by sending a further message, e.g. a ready to receive message, from the target to the initiator.

With this invention it is possible to prevent an denial-of-service attack in a network caused by a multitude of requests sent to a target from an initiator using a false sourceID.

According to a preferred embodiment, the method according to the invention is embedded in a 3-way handshake protocol.

Advantageously, the steps of generating the question and evaluating the answer are performed in a separate module. This separate module can be incorporated into a hardware module, such as a logic chip, PLD or FPGA, resulting in high processing speed.

Preferably, the question sent to the initiator comprises parameters associated with the sourceID and the target. This question can be encrypted in order to further increase reliability of the method according to the invention.

According to a preferred embodiment, the method according to the invention further comprises the step of entering initiator related information in a table. Therefore, it is possible to observe the number of connections between a certain ini-

tiator and a target or alternatively, the number of requests. As soon as the observed number of connections or requests exceeds a predetermined value, no more connections are established to prevent flooding of the target by the certain initiator.

Advantageously, the network is an InfiniBand network offering high speed and great performance.

Furthermore, the invention covers a module for protecting a target against attacks in a high-speed network comprising means for generating a question triggered by a request and means for evaluating an answer to this question.

Preferably, this module is incorporated into a hardware module, such as a logic chip, PLD or FPGA. This hardware module can be integrated into a network adapter housing or alternatively, into a separate housing.

According to another embodiment, the module is incorporated into a software module preferably, running on a separate processor.

The invention also covers a computer program product with a computer-readable medium and a computer program stored on said computer-readable medium with program coding means which are suitable for carrying out a method according to the invention when said computer program is run on a computer.

Moreover, the invention covers a method for handling a request in a high-speed network at a target using a common handshake protocol, wherein as soon as the load of the target caused by processing of requests exceeds a predetermined

threshold value, the common handshake protocol is amended by a method according to any one of claims 1 to 8.

As the protection against request flooding is only needed in high utilization times, the common handshake protocol, typically an 3-way handshake protocol, can be used in low utilization times. The handshake protocol according to the invention introduces two additional steps and is used in high utilization times.

Further features and embodiments of the invention will become apparent from the description and the accompanying drawings.

It will be understood that the features mentioned above and those described hereinafter can be used not only in the combination specified but also in other combinations or on their own, without departing from the scope of the present invention.

The invention is schematically illustrated in the drawings by way of example and is hereinafter explained in detail with reference to the drawings. It is understood that the description is in no way limiting on the scope of the invention and is merely an illustration of preferred embodiments of the present invention.

BRIEF DESCRIPTION OF THE DRAWINGS

Other aspects and advantages of the invention will become apparent upon review of the detailed description and upon reference of the drawings in which:

Figure 1 shows a possible scenario for a denial of service attack,

Figure 2 shows a diagram explaining a 3-way handshake protocol,

Figure 3 shows a diagram explaining a 4-way handshake protocol in a TCP network,

Figure 4 shows a diagram explaining the 4-way handshake protocol in an InfiniBand network,

Figure 5 shows a diagram illustrating the 5-way handshake protocol in an InfiniBand network according to the present invention,

Figure 6 is a block diagram schematically showing a module according to the invention in a network environment,

Figure 7 shows a diagram explaining handling of a request in a network according to the invention and contains naming for Figure 8, and

Figure 8 is a flow chart illustrating the method according to the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

A possible scenario for a denial-of-service attack is shown in Figure 1. An attacker 10 using the sourceID of an authorized initiator 12 sends an request to a target 14 via a fabric 16. According to the invention, this request is evaluated in a hardware networking module 18 to make sure that the resources of main CPUs 20 in the target are not consumed and flooding of the target is prevented.

Referring to Figure 2, a 3-way handshake protocol is illustrated. An initiator defined by a sourceID sends a request message to a target identified by a destinationID. The target sends back a ready to receive message including target parameters. To establish the connection the initiator transmits a ready to receive message containing initiator parameters.

Using the 3-way handshake protocol an attacker utilizing a counterfeit address can flood the target with connection requests, since the target allocates resources before identification of the initiator is performed.

Referring to Figure 3, a 4-way handshake protocol in a TCP network is shown. After having received a request from a initiator the target sends a question to the initiator which allocates resources. The initiator transmits an answer to the question together with a ready to receive message including initiator parameters. The target evaluates the answer and in case that it is a valid answer, sends back a ready to receive message to establish the connection. Consequently, the resource allocation is performed after identification of the initiator.

However, as illustrated in Figure 4, the 4-way handshake protocol does not solve the request flooding attack problem in an InfiniBand network, since a non-transparent sequence change of I -> T and T -> I is caused, that is not transparent to upper layer protocols. As the I -> T and T messages contain upper layer connection establishment parameters and QPNs, this approach is not feasible for an InfiniBand network. The problem is, that the target does not know when sending is allowed. Furthermore, this approach does not solve the problem in connection with the limited number of possible queue pair numbers.

Referring to Figure 5, a 5-way handshake protocol according to the invention is embedded in a 3-way handshake protocol. After having received a request from an initiator identified by a sourceID a target preferably, a hardware module associated with the target generates a question derived from the sourceID which does not include persistent data to the node identified by the sourceID. Consequently, an attacker using a counterfeit address does not receive this question and therefore, cannot answer the question. In case that a valid sourceID was used, the target answers the question. This answer is evaluated by the target. If the answer matches, the connection is established.

The question generation and answer check is performed without involving the software of the target. No pesistent data must be stored in the target between the question and the answer. Moreover, the approach is transparent for upper level protocols and backward compatible in normal situations.

According to Figure 6, a connection HW assist module 30 is connected to a send buffer 32 which contains the outgoing messages before they are transmitted. A SERDES 34 reads all incoming messages which are stored in a receive buffer 36. The module 30 is connected to a control logic 38 to trigger "Forward message" and "drop message" operations and to signal "additional high load information", e.g. arrival of a connection request with source address or the arrival rate. A load detection module 40 containing a table comprising initiator related data signals "normal operation", high load" and "drop all connection requests from a verified initiator" to the connection HW assist module.

The proposed 5-way handshake protocol is an effective solution for preventing flooding of a target. As the protection against request flooding is only needed in high utilization times, the 3-way handshake may be used in low utilization times. The 5-way handshake introduces two additional messages, the question or challenge, respectively and the challenge response.

Referring to Figure 7, an initiator using a sourceID sends a request R to a target for establishing a connection. The target generates a questions Q=f(...) which is transmitted to the entity identified by the sourceID contained in R via a switch network. Only an entity receiving Q is able to create an answer A which is sent back to the target. The switch network transports A to the target based on the destinationID contained in Q. The target validates, if the creator of A has seen Q by g(A,...). In a preferred embodiment Q=f(sourceID, key,...) and valid=g(A, sourceID, key,...).

Results of f should be hard to predict by any initiator without knowing "key" (plaintext cipher attack, freely chooseable plaintext), e.g. use of a regularly changed key. The key generation must not be predictable by any initiator, e.g. use of physical noise to generate key. Furthermore, different initiators must lead to different keys, e.g. by use of InfiniBand LID, GID, GUID as input parameters. The target decides based on A and "key", whether the answer A has been sent by the initiator the address of which matches Q.

In an alternate implementation, the question message could be an InfiniBand redirection message (GetResp(ClassPortInfo)) containing InfiniBand parameters to be used for the answer. The answer is a repeated connection establishment message (InfiniBand REQ) with the original set of parameters except

from the parameters specified in the question message (GetResp(ClassPortInfo) All parameters capable for redirection can be used to form the question message.

Referring to Figure 8, a module associated with a target to be protected waits for an incoming message (step 50). Having received a message, the header of said message is analysed in step 52. If the received message is a request for a connection 54, a question is generated in step 56 and sent to the node identified by the received sourceID (step 58).

If the received message is an answer 60, this answer is evaluated in step 62. In case that the answer is valid, the message is forwarded to the target (step 64). If not, the message is dropped (step 66).

If the received message is neither a request nor an answer 68, the message is forwarded to the target (70).

Claims

What we claim is:

1. A method for protecting a target against attacks in a high-speed network comprising the steps of:

- after having received a request from an initiator identified by a sourceID associated to a certain node in the network generating a question,
- sending the question to the node identified by the sourceID,
- in case that an answer to the question is received, evaluating the answer,
- in case that a proper answer has been received, enabling communication between the initiator and the target by sending a further message from the target to the initiator.

2. A method according to claim 1, wherein said method is embedded in a 3-way handshake protocol.

3. A method according to claim 2, wherein the steps of generating the question and evaluating the answer are performed in a separate module.

4. A method according to claim 3, wherein the separate module is incorporated into a hardware module.

5. A method according to claim 1, wherein the question comprises parameters associated with the sourceID and the target.

6. A method according to claim 1, further comprising the step of encrypting the question.

7. A method according to claim 1, further comprising the step of entering initiator related information in a table.

8. A method according to claim 1, wherein the network is an InfiniBand network.

9. A module for protecting a target against attacks in a high-speed network comprising means for generating a question triggered by a request and means for evaluating an answer to this question.

10. A module according to claim 9 incorporated into a hardware module.

11. A module according to claim 10, wherein said module is integrated into a network adapter housing.

12. A module according to claim 10, wherein said module is integrated into a separate housing.

13. A module according to claim 10 incorporated into a software module.

14. A computer program product with a computer-readable medium and a computer program stored on said computer-readable medium with program coding means which are suitable for carrying out a method according to any one of claims 1 to 8 when said computer program is run on a computer.

15. A computer program with program coding means which are suitable for carrying out a method according to any one of

claims 1 to 8 when said computer program is run on a computer.

16. Method for handling a request in a high-speed network at a target using a common handshake protocol, wherein as soon as the load of the target exceeds a predetermined threshold value the common handshake protocol is amended by a method according to any one of claims 1 to 8.

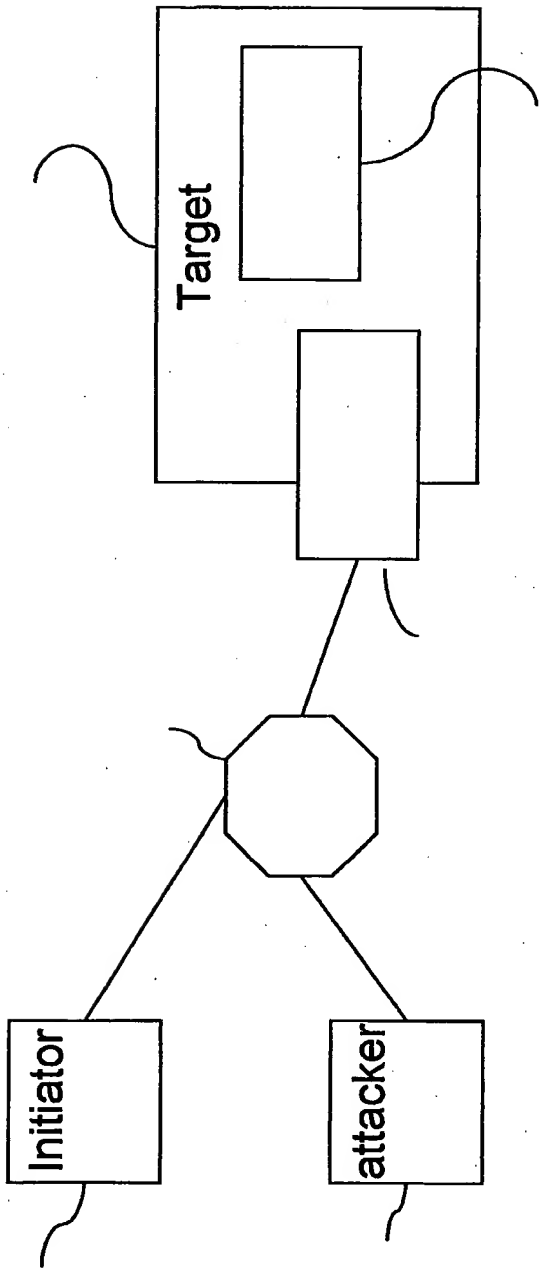


Fig. 1

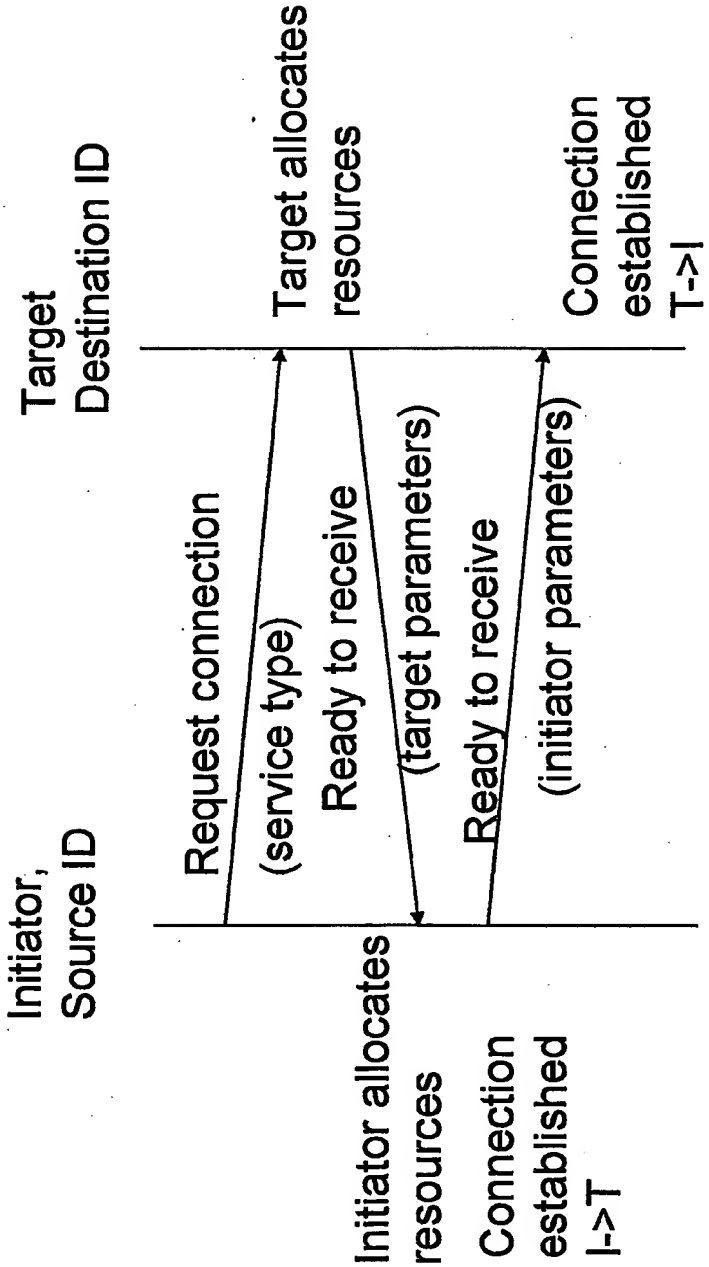

Initiator,
Source ID
Target
Destination ID
Request connection
(service type)
Ready to receive
(target parameters)
Ready to receive
(initiator parameters)
Target allocates
resources
Connection
established
T->I
Initiator allocates
resources
Connection
established
I->T

Fig. 2

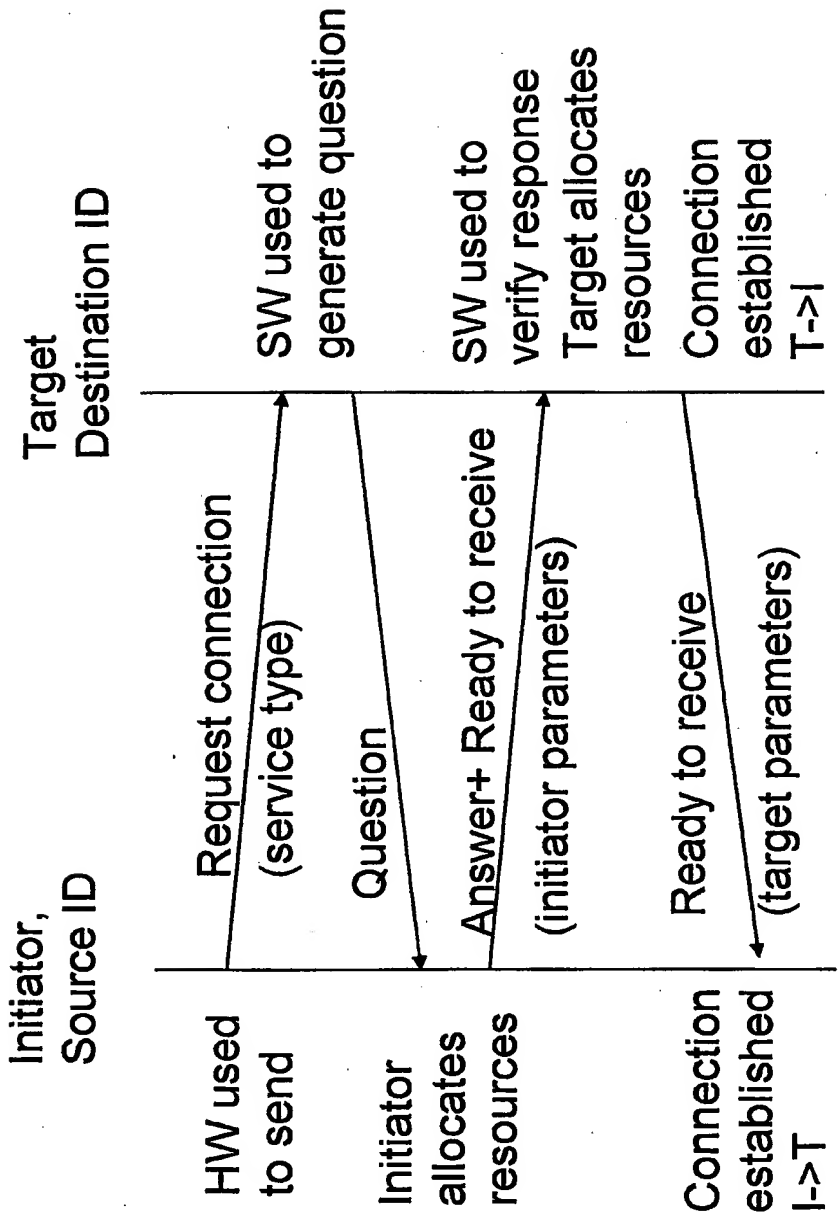

Initiator,
Source ID
Target
Destination ID
HW used
to send
Request connection
(service type)
SW used to
generate question
Question
Initiator
allocates
resources
Answer+ Ready to receive
(initiator parameters)
SW used to
verify response
Target allocates
resources
Connection
established
I->T
Ready to receive
(target parameters)
Connection
established
T->I

Fig. 3

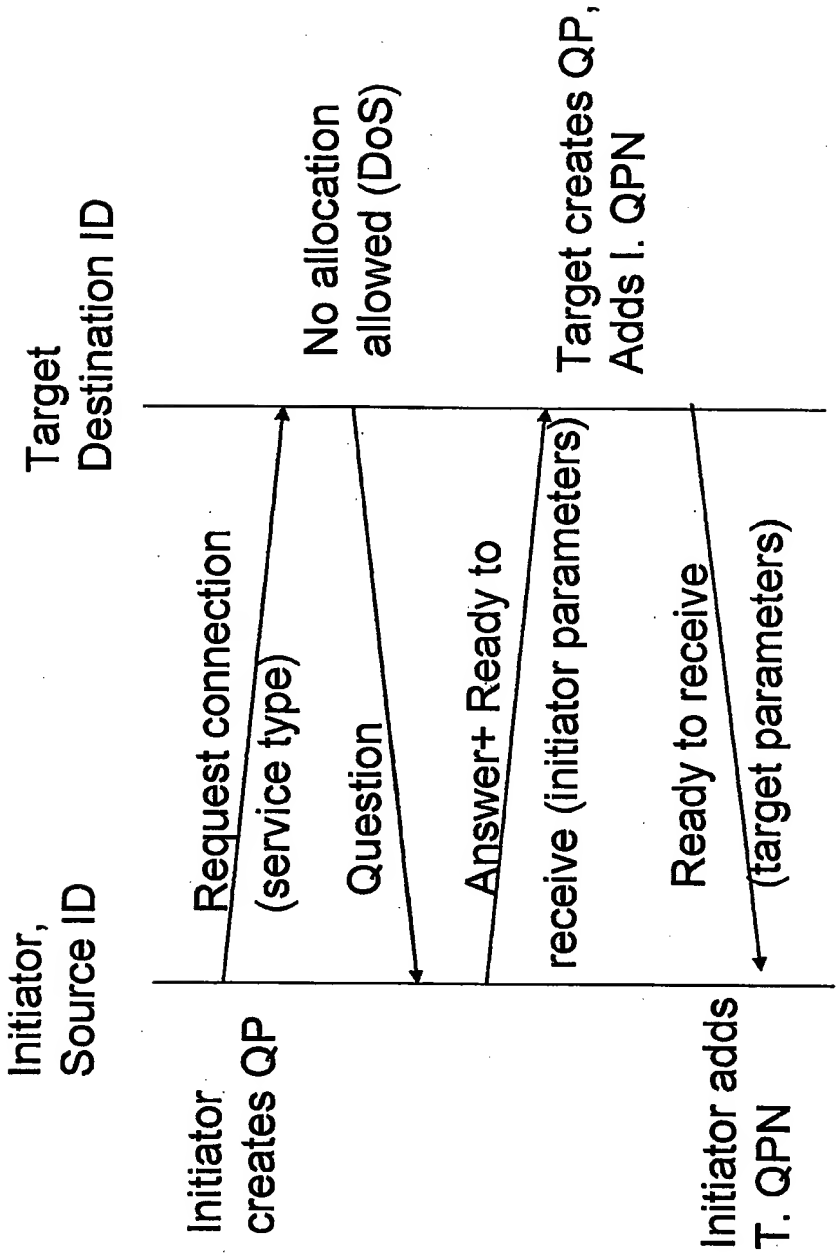

Initiator,
Source ID
Target
Destination ID
Initiator
creates QP
Request connection
(service type)
No allocation
allowed (DoS)
Question
Target creates QP,
Adds I. QPN
Answer+ Ready to
receive (initiator parameters)
Ready to receive
(target parameters)
Initiator adds
T. QPN

Fig. 4

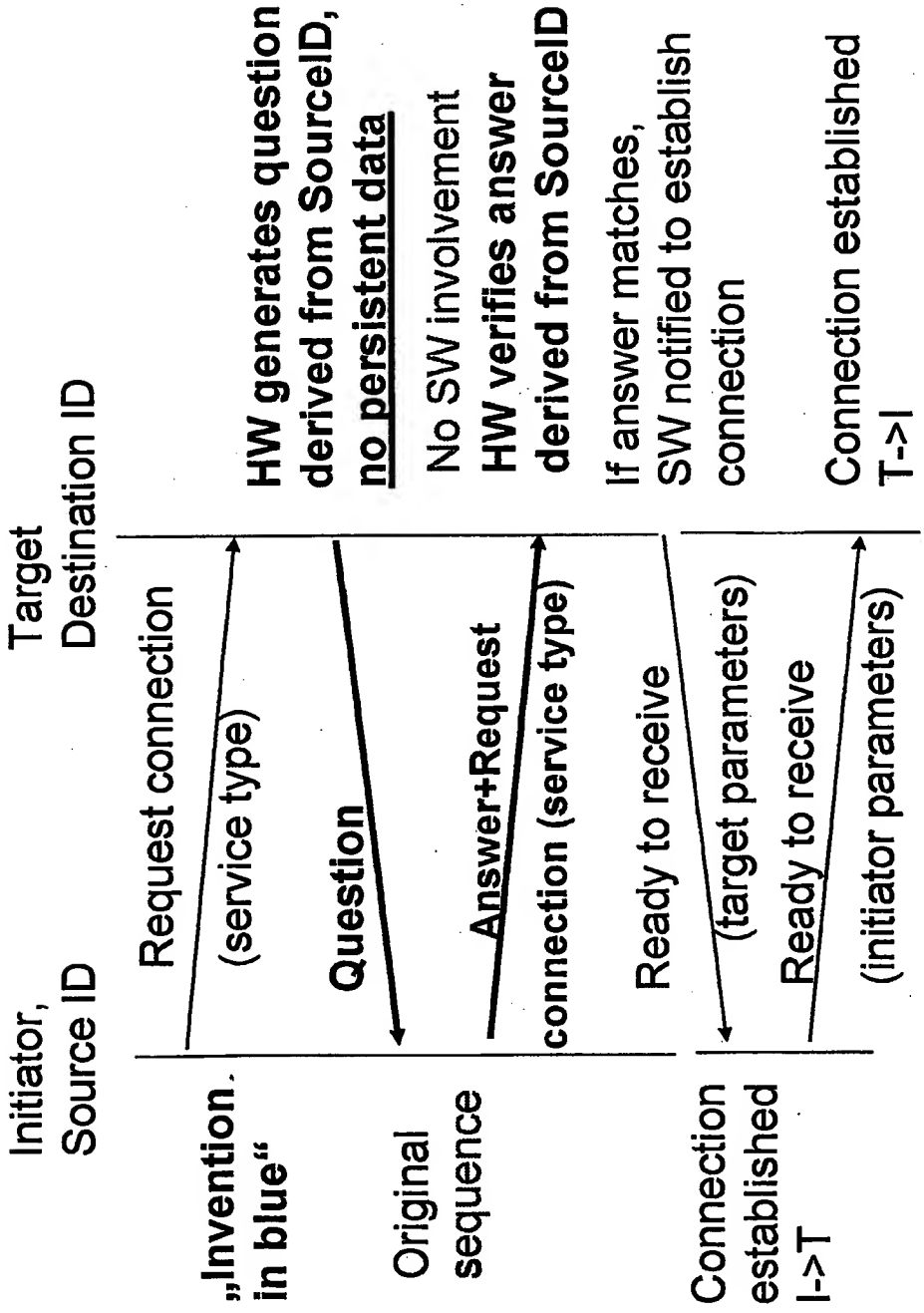

Initiator, Source ID
Target Destination ID
„Invention. in blue“
Original sequence
Connection established I->T
Request connection
(service type)
Question
Answer+Request connection (service type)
Ready to receive
(target parameters)
Ready to receive
(initiator parameters)
HW generates question derived from SourceID, no persistent data
No SW involvement
HW verifies answer derived from SourceID
If answer matches, SW notified to establish connection
Connection established T->I

Fig. 5

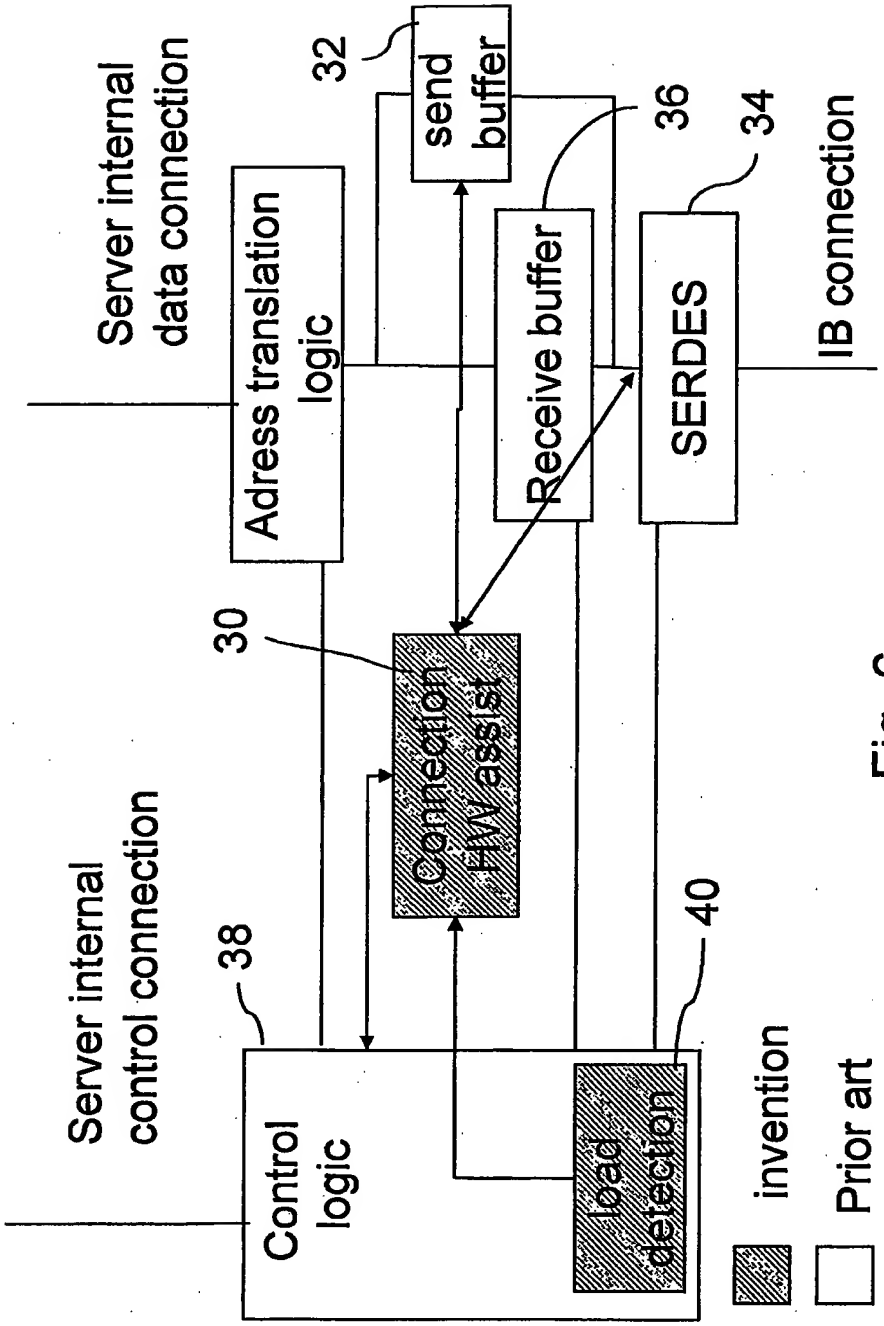

Server internal data connection
Server internal control connection
Adress translation logic
send buffer
Receive buffer
SERDES
IB connection
Connection HW assist
Control logic
load detection
32
36
34
30
38
40
invention
Prior art

Fig. 6

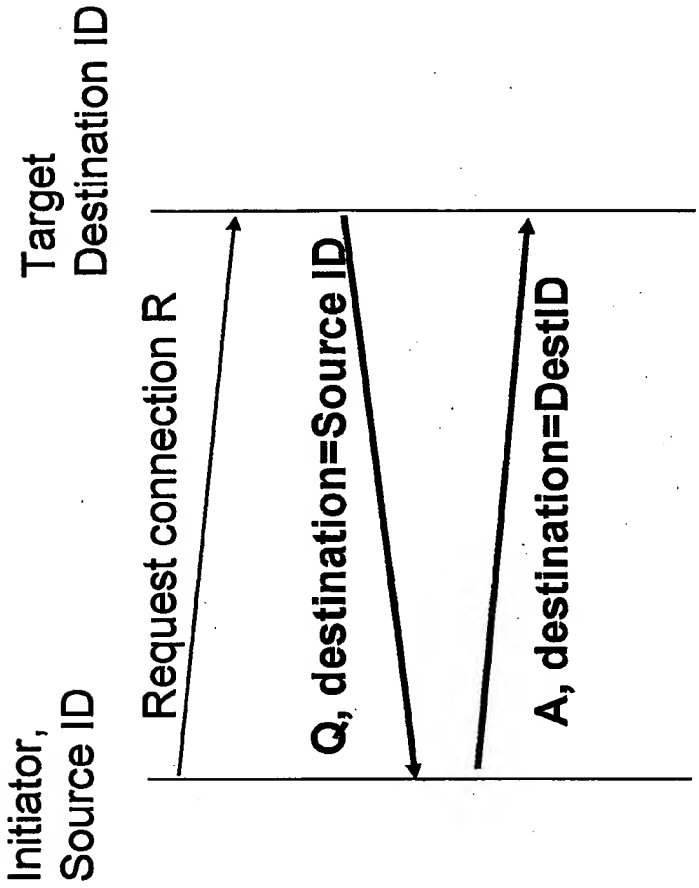

Initiator,
Source ID
Target
Destination ID
Request connection R
Q, destination=Source ID
A, destination=DestID

Fig. 7

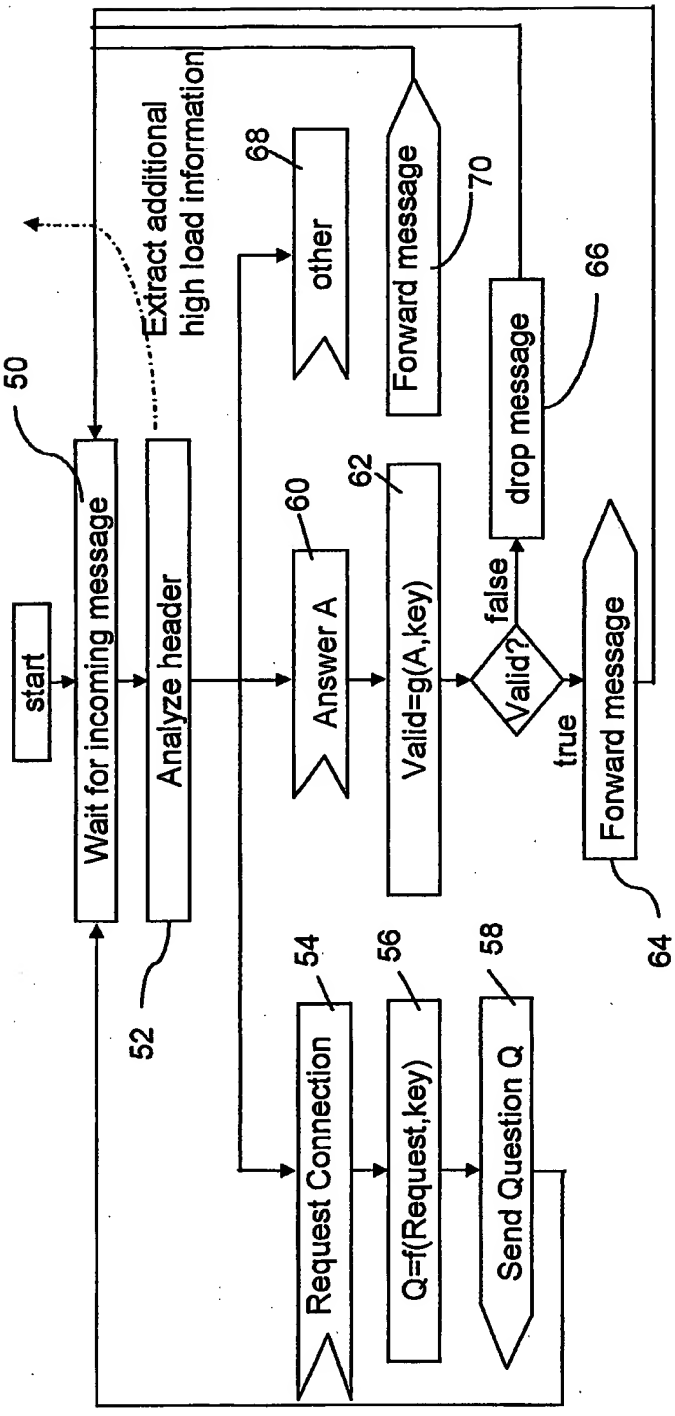

start
Wait for incoming message
50
Analyze header
52
Extract additional high load information
Answer A
60
Valid=g(A,key)
62
Valid?
false
true
drop message
66
Forward message
64
other
68
Forward message
70
Request Connection
54
Q=f(Request,key)
56
Send Question Q
58

Fig. 8

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/051546

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	ARI JUELS AND JOHN BRAINARD: "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks" PROCEEDINGS OF NDSS '99 (NETWORKS AND DISTRIBUTED SECURITY SYSTEMS), 'Online! 3 February 1999 (1999-02-03), pages 151-165, XP002340691 Retrieved from the Internet: URL:http://www.rsasecurity.com/rsalabs/staff/bios/ajuels/publications/client-puzzles/clientpuzzles.ps> 'retrieved on 2005-08-12! Abstract 3.3 Client puzzle protocol description -/--	1-16

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 August 2005	26/08/2005

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bertolissi, E

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/EP2005/051546

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2002/073322 A1 (PARK DONG-GOOK ET AL) 13 June 2002 (2002-06-13) abstract paragraph '0046! - paragraph '0063! figures 3,4	1-16
X	AURA T ET AL: "DOS-Resistant Authentication with Client Puzzles" SECURITY PROTOCOLS. INTERNATIONAL WORKSHOP PROCEEDINGS, 2000, pages 170-177, XP002275098 Abstract 3 Client puzzles	1-16
X	GERAINT PRICE: "A General Attack Model on Hash-Based Client Puzzles" SPRINGER-VERLAG LECTURE NOTES IN COMPUTER SCIENCE : CRYPTOGRAPHY AND CODING, 'Online! November 2003 (2003-11), pages 319-331, XP002340692 Retrieved from the Internet: URL:http://www.springerlink.com/media/G275MUNQVQ2YXP5VUXV2/Contributions/H/B/9/D/HB9D37D7TC0GBCTV_html/BodyRef/PDF/558_10966013_Chapter_26.pdf> 'retrieved on 2005-08-12! Abstract sections 2, and 4	1-16
A	STUBBLEFIELD, A., AND D. DEAN: "Using Client Puzzles to Protect TLS" PROCEEDINGS OF THE TENTH USENIX SECURITY SYMPOSIUM, 'Online! 13 August 2001 (2001-08-13), XP002340693 Washington, DC Retrieved from the Internet: URL:http://www.csl.sri.com/users/ddean/papers/usenix01b.pdf> 'retrieved on 2005-08-12! Abstract Section 3	1-16
A	KARTHIK LAKSHMINARAYANAN, DANIEL ADKINS, ADRIAN PERRIG AND ION STOICA: "Taming IP packet flooding attacks" 2ND WORKSHOP ON HOT TOPICS IN NETWORKS (HOTNETS-II), 'Online! 20 November 2003 (2003-11-20), XP002340694 Retrieved from the Internet: URL:http://i3.cs.berkeley.edu/i3/publications/papers/hotnets03.pdf> 'retrieved on 2005-08-16! Abstract Section 4	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/EP2005/051546

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2002073322 A1	13-06-2002	KR 2002045003 A	19-06-2002